Attorney's Docket No. 032326-133

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	MAIL STOP AMENDMENT
Christophe Clavier et al.	Group Art Unit: 2131
Application No.: 09/807,615	Examiner: Syed Zia
Filed: July 13, 2001	Confirmation No.: 2076
For: COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM	

REQUEST FOR RECONSIDERATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated June 30, 2005, Applicants respectfully request reconsideration and withdrawal of the rejections of the claims.

Claims 11-15 were rejected under 35 U.S.C. § 102, on the grounds that they were considered to be anticipated by the Kocher et al patent (US 6,278,783). The Kocher patent, like the present invention, is concerned with an attacker's ability to derive secure information by observing a series of operations performed in a cryptographic system. However, the approach that is employed in the Kocher patent is substantially different from the claimed invention. Specifically, the Kocher patent discloses a technique wherein the message to be encrypted, and/or the encryption keys, are disguised, or "blinded", prior to processing by the DES algorithm. This blinding is accomplished by generating two values which, when combined with one another by means of an exclusive-or operation, result in the original message, or keys. Permutations of these values are employed to perform the encryption.

It is respectfully submitted that this disclosure does not anticipate the subject matter of claims 11-15. With respect to claim 11, the Office Action states that the Kocher patent discloses a program memory having stored therein a plurality of manipulating means for use during critical instructions, with reference to column 2, lines 25-36. This portion of the patent